

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 02-041051

(43)Date of publication of application : 09.02.1990

(51)Int.Cl. H04L 9/06
 H04H 1/00
 H04L 9/14
 H04N 7/167

(21)Application number : 63-191781

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
 KONDEISHIYONARU AKUSESU TECHNOL
 KENKYUSHO:KK

(22)Date of filing : 29.07.1988

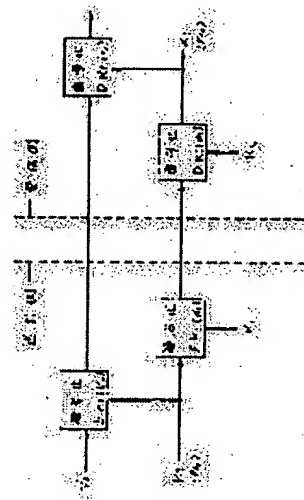
(72)Inventor : HIRASHIMA MASAYOSHI
 SATO TOSHICHIKA

(54) RECORDING SYSTEM

(57)Abstract:

PURPOSE: To attain the decoding of recording information for a specific cryptographic decoder only by ciphering a key K_t to decode cryptographic information by a key K_i specific to each decoder so as to form a key $E_{K_i}(K_t)$ and recording it together with cryptographic information.

CONSTITUTION: Suppose that a video signal and a voice signal are scrambled by using a function $f(K_t)$ decided definitely with a key K_t changing as time elapses, then in the case of sending the key K_t from the sender side to the receiver side, since the possibility of interception exists without any modification, the key is ciphered by other key K_i to form a key E_{K_i} and it is recorded on a VTR or the like together with cryptographic information. When the recorded information is reproduced, since the key $E_{K_i}(K_t)$ is obtained, the result $D_{K_i}(K_t)$ being the decoding of the $E_{K_i}(K_t)$ is decoded by using further the key K_i to obtain the key K_t , and then the reproduced scrambling information signal is decoded.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the
 examiner's decision of rejection or application
 converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of
 rejection]

[Date of requesting appeal against examiner's decision
 of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

⑫ 公開特許公報(A)

平2-41051

⑮ Int. Cl.³

識別記号

庁内整理番号

⑬ 公開 平成2年(1990)2月9日

H 04 L 9/06
H 04 H 1/00
H 04 L 9/14
H 04 N 7/167

F 7608-5K

8725-5C

7240-5K

H 04 L 9/02

Z

審査請求 未請求 請求項の数 7 (全8頁)

⑭ 発明の名称 記録システム

⑰ 特 願 昭63-191781

⑱ 出 願 昭63(1988)7月29日

⑲ 発 明 者 平 嶋 正 芳 大阪府門真市大字門真1006番地 松下電器産業株式会社内
⑲ 発 明 者 佐 藤 寿 親 大阪府門真市大字門真1006番地 松下電器産業株式会社内
⑲ 出 願 人 松下電器産業株式会社 大阪府門真市大字門真1006番地
⑲ 出 願 人 株式会社コンディショ 東京都港区虎ノ門1丁目19番地10号
ナル・アクセス・テク
ノロジー研究所
⑲ 代 理 人 弁理士 栗野 重孝 外1名

明 細 書

1、発明の名称

記録システム

2、特許請求の範囲

- (1) 階層構造をとる複数の鍵により記録データを暗号化及び復号化する記録システムであって、暗号化した映像信号と一定の時間を経過した時に更新される鍵 K_t を含む制御信号とを同一の記録媒体上に記録するに際し、上記鍵 K_t をシステム中の暗号解読装置に固有な鍵 K_1 を用いて暗号化した $E_{K_1}(K_t)$ として記録するようにしたことを特徴とする記録システム。
- (2) 鍵 K_t より更新周期の長い鍵 K_x を鍵 K_t と共に用いるようにし、鍵 K_t を鍵 K_x で暗号化し、鍵 K_x を鍵 K_1 で暗号化して、 $E_{K_1}(K_x)$ の形で記録するようにしたことを特徴とする請求項1記載の記録システム。
- (3) 信号送出側から送られてくる鍵 K_t の送出形式と同一の形式で、暗号解読装置から $E_{K_1}(K_t)$ を解読した $D_{K_1}(K_t)=K_t$ を出力し、同時に映像信号

と音声信号を再生して出力するようにしたことを特徴とする請求項1記載の記録システム。

(4) 信号送出側から送られてくる鍵 K_x の送出形式と同一の形式で、暗号解読装置から $E_{K_1}(K_x)$ を解読した $D_{K_1}(K_x)=K_x$ を出力し、同時に映像信号と音声信号を再生して出力するようにしたことを特徴とする請求項2記載の記録システム。

(5) 記録される信号が鍵 K_t により暗号化されていることを特徴とする請求項1、または3記載の記録システム。

(6) 記録される信号が鍵 K_t により暗号化されていることを特徴とする請求項2または4項記載の記録システム。

(7) 有料視聴デコーダ内において、記録された信号を再生して得られる復号化用の制御信号の処理回路と、放送局から送られて来る信号中の復号化用の制御信号の処理回路とを部分的に共通にするとともに、両回路の切替えを外部から行うことを物理的に阻止する構造にしたことを特徴とする請求項1～6のいずれかに記載の記録システム。

3. 発明の詳細な説明

産業上の利用分野

本発明は、情報を暗号化して記録し、特定の再生装置によってのみ再生できるようにする記録システムに関する。

従来の技術

情報（映像・音声・データ）を暗号化して伝送・受信することは従来から知られているが、暗号化する場合、秘密を保ちたい情報と、料金を支払った者だけに見せる情報とがある。秘密を保ちたい場合は情報を暗号化したままの状態記録するようにすればよいが、その場合にはどの暗号復号装置でも解読できるというのでは望ましくない。また、有料の場合は、解読された情報がコピーされること望ましくない。

本発明は、これらの課題を解決する記録システムに関する技術である。

発明が解決しようとする課題

従来の記録システムにおいては、暗号化したまま記録する場合であっても、どの復号装置でも

解読できるという問題があった。

また、暗号化された情報を解読して記録する場合は例えば機器の密番を符号化して同時に記録していたが、解読された情報のコピーを防ぐことができないという問題があった。

そこで、本発明はかかる従来の問題を解消して、特定の暗号復号器でのみ記録情報を解読することができ、また、解読された情報のコピーを防止することもできる記録システムを提供することを目的とする。

課題を解決するための手段

この目的を達成するため、本発明においては、暗号化情報を解読するための鍵 K_t 又は K_x を各々の解読装置に固有の鍵 K_i で暗号化して $E_{K_i}(K_x)$ とし、暗号化情報とともに記録するようにした点に特徴がある。従って、記録された情報をそのまま再生しても暗号化されたままであり、記録に用いられた鍵 K_i を有する暗号解読装置によってのみ解読できる。

作 用

このような本発明によると、一般には鍵 K_t 又は K_x は時間が経過すると変化するので、再生時に暗号解読装置の鍵 K_t 又は K_x が情報信号を記録した時とは異なっていると、再生した時にスクランブル化された映像や音声等の暗号化情報が復元できないが、本発明の記録システムによれば、記録した情報信号を再生したときに $E_{K_i}(K_t)$ 又は $E_{K_i}(K_x)$ が得られるので、これを解読した $D_{K_i}(K_t)$ 又は $D_{K_i}(K_x)$ をさらに鍵 K_i で解読することにより K_x を得て、再生したスクランブル化情報信号を解読（デスクランブル化）することができる。

実 施 例

本発明の一実施例を第1図に示す。図中、1～6の部分記録再生部（たとえばVTR）であり、11～21、29の部分は暗号解読機能及び暗号化機能を含む有料デコーダの一部を示す。

第1図中、入力バッファ回路1、3、映像記録ヘッド4、音声記録ヘッド5は通常のVTRの該当部分と共通の回路等である。また、データ抜取回路14、暗号復号化回路15、鍵 K_t メモリ16は、

既に実用化されている有料放送（例えばVideo Clipper IIやBMAC等）の有料デコーダの当該部分と機能的に同一の回路である。

まず、本発明の記録システムの基礎となる暗号化システム全体の概要を第2図、第3図を参照して説明する。ここでは、時間の経過により変化する鍵 K_t によって一義的に決まる関数 $f(K_t)$ により映像信号及び音声信号をスクランブル化するものとする。鍵 K_t を送出側から受信側へ伝送する場合。そのままの形では盗聴されるおそれがあるので、別の鍵 K_i で暗号化する。鍵 K_i は、端末1台ずつに別々のものを割当てても、数台まとめて一の鍵を割当てても、全端末に共通の鍵を使用してもよい。このような鍵の重層構造については、たとえば、一松信監修「データ保護と暗号化の研究」第63頁図1-27、等に記載されている。鍵 K_t と K_i の間に、もう一つ鍵 K_x より長い周期で更新される鍵 K_x を用いてもよい。このことも同文献に示されている。第3図がその例である。

ここでは、説明を簡単にするために、第2図の

場合について説明する。放送の形式として、鍵等の制御信号をデジタル信号で送出できる放送衛星BS2で採用されている方式を考える。この方式は、^{その}音声をデジタル信号で伝送するので、音声データにPN信号を加算すれば暗号化(スクランブル化)できる。従って、そのPN信号の初期値がすなわち鍵 K_t となり、これが判れば復号化(デスクランブル化)できる。この鍵 K_t を鍵 K_t で暗号化(スクランブル化)して送り、受信側で鍵 K_t で復号化すればよい。映像信号については、ラインローテーションによる暗号化(スクランブル化)を行ない、その各ラインでの切断点を上記PN信号で与えればよく、これについては公知の技術が使える。

さて、第1図において、 P_1 は受信側での受信信号の入力端子で、例えばBSチューナのFM検波複合映像出力信号をそのまま入力すればよい。11は入力バッファ回路、12は5.73MHzの音声搬送波成分と映像信号成分とを分離する分離回路、13は5.73MHzのQPSK信号を復調し2.048

VTRの記録帯域が狭い場合には音声データ信号をベースバンドで記録すればよいが、ベースバンドの音声データ信号をスクランブル化して記録するためには、有料デコーダ側に音声スクランブル化回路が必要になる。このことは、本発明の主題ではないので、ここでは、VTRで4.5MHzまで記録できるものとしておく。

一方、メモリ16に記憶された鍵 K_t は暗号化回路19でメモリ29からの端末固有の鍵 K_t (ここでは、1端毎に鍵 K_t が異なるものとする)で暗号化し、出力バッファ回路20を介して出力端子 P_3 より出力する。暗号化回路19及び出力バッファ回路20はそれぞれの内部にバッファメモリを有するものである。

今、第4図に示す時刻 t_0 にVTRの記録開始制御回路2で記録開始を指示すると、 ϕ_0 の制御信号が、1、3、4、6の各回路へ伝えられ、有料デコーダの出力端子 P_2 、 P_3 からの出力信号を同一のテープに記録する。次に、有料デコーダ側で時刻 t_1 に切換スイッチ22を操作すると、R/W制御

Mbpsのデジタル信号を得る復調回路である。14はQPSK復調回路13の出力から音声データ以外の制御信号データを抜取りる抜取回路、15はその制御信号データから暗号化されている鍵 K_t その他の信号を復号する復号化回路、16は復号化回路15の出力中の鍵 K_t を記憶するメモリAである。なお、メモリA16の他に鍵 K_t 以外の制御信号を記憶するメモリが別にあることはいうまでもない。

一方、17は4.5MHzの連続搬送波を2.048Mbpsの音声データで振幅変調する変調回路であり、変調回路17の変調音声出力と分離回路12の映像信号成分出力とを混合回路18で混合し、出力端子 P_2 より出力する。従って、出力端子 P_2 の出力信号は地上テレビ放送のNTSC方式のテレビ信号と類似のものとなり、AM変調された4.5MHzの音声データ信号が含まれていることになる。

この信号がVTRの入力バッファ回路1を介して映像記録ヘッド4でテープに記録される。この場合、映像記録ヘッド4は4.5MHz以上の高域まで記録可能であることはいうまでもない。なお、

回路21から制御信号 ϕ_1 (ϕ_{11})、 ϕ_2 (ϕ_{12})が出力され、メモリ16から鍵 K_t を読み出して暗号化回路19へ入力し、暗号化回路19で鍵 K_t により暗号化して EK_t (K_t)として出力バッファ回路20へ伝え、そのバッファメモリへ書込む。この作用が $t_1 \sim t_2$ の間に終り、続いて $t_2 \sim t_3$ の間に出力バッファ回路20から1200bpsの低速でその EK_t (K_t)を読み出し、出力端子 P_3 から出力する。その信号の形式をデータ抜取回路14で抜取った出力と同じバケット構造とし、1バケットを272ビットとする。ここでは出力バッファ回路20から EK_t (K_t)を1200bpsでフレイズエンコードして読み出すものとするれば、約0.23秒で272ビットのデータを出力することができる。これをVTRの入力バッファ回路3を介して音声記録ヘッドで音声トラックに記録する。VTRの音声トラックの記録帯域は、5KHz以上あり、1200bpsで読出されるデータをフレイズエンコードして得られる出力信号の最高周波数成分より十分高域まで伸びているので、記録上の問題はな

い。このようにしてVTRのテープの音声トラックに $EK_i(K_t)$ を記録する場合、最初に1回だけ ϕ_2 の如く $t_2 \sim t_3$ の間のみ記録する場合と、 ϕ_{12} の如く一定間隔で $t_{n2} \sim t_{n3}$ の間にくり返し記録する方法があるが、どちらでもよい。その記録制御用の信号 ϕ_1 又は ϕ_{11} はR/W制御回路21で形成し、切換スイッチ22の設定により切換える。

以上の如く構成すれば、第4図の記録制御信号 ϕ_0 が高レベルの間に暗号化されている映像信号(音声コード信号を含む)をVTRに映像記録ヘッド4により記録し、かつ鍵 K_t も暗号化して $EK_i(K_t)$ としてVTRの音声トラックに音声記録ヘッド6により記録することができる。この場合、記録再生部のVTRとして既存のVTRを使うことができる。なお、VTRにおける映像信号の記録帯域幅が広ければ変調回路17を用いずに入力バッファ回路11の出力を直接出力端子 P_2 へ出力し、そのまま映像記録ヘッド4へ伝えて記録することも可能である。

給する。これにより、 K_t メモリA10はその出力がハイインピーダンスとなり、保持状態となり、他方の K_t メモリB30が能動状態になる。また、このときセレクト20はQPSK復調回路13の出力に代えて音声検波回路25の出力をデータ処理回路14へ加える。従って、データ処理回路14にはQPSK復調回路13の出力と同形式の音声検波回路25の出力が加える。このデータ処理回路14は、QPSK復調回路13の出力も音声検波回路25の出力も同じように処理する。そして、暗号復号回路15でデータ中の一部の制御信号の暗号を解読する。この15の動作については後述する。暗号復号回路15の出力中の鍵 K_t 以外の情報はデスクランブル処理部32へ伝える。

デスクランブル処理部32では鍵 K_t を用いてデータ抜取回路14の出力の一部(暗号復号回路15で解読していない部分)の解読を行ない、復号化(デスクランブル)について必要な情報を得、その情報に基づき再生信号をデスクランブルする。音声データ信号の復号化(デスクランブル)は音

次に、このようにして記録された映像・音声信号と鍵との再生について、第5図を参照して説明する。第4図で説明したように、再生信号の始めの部分の $t_2 \sim t_3$ のみに $EK_i(K_t)$ が記録されている場合と、 $t_{n2} \sim t_{n3}$ にくり返して記録されている場合があるが、どちらでも同じように動作する。まず、記録再生部の再生開始制御回路10で再生開始を制御すると、音声再生ヘッド7で音声トラックから暗号化した $EK_i(K_t)$ のフェイズエンコード信号を再生し、出力バッファ回路9を介して有料デコーダの入力端子 P_5 に入力する。入力バッファ回路27でその出力信号をフェイズデコードして1200bpsの272ビットのデジタル信号 $EK_i(K_t)$ に戻す。その入力バッファ回路27の出力 $EK_i(K_t)$ をメモリ29に記憶されている端末固有の鍵 K_i で復号化(デコード)して鍵 K_t を得る。この鍵 K_t を K_t メモリB30に蓄込む。

一方、このときVTR再生指示回路31から再生指示信号を発して K_t メモリA10、セレクト20、 K_t メモリB30、デスクランブル処理部32へ供

声データのフレーム周期の初めに所定のPN初期値即ち鍵 K_t を与えてPN系列を発生させ、そのPN値をデータ処理部14の出力の音声データ信号に加算することによって行なう。

映像信号については、その暗号化の際にラインローテーションのカット位置をPN値で指定し、例えば第22ライン目のカット位置を鍵 K_t 則ちPNの初期値で指定し、以下、第23、24……202ライン目までPN系列の示す位置で1ラインの映像信号をカットしローテーションする。このとき、毎フィールド又は毎フレームでの同じラインは同じ位置でカットする。ラインローテーション前のあるライン映像信号の波形が第8図Aに示すようなものであったとすれば、所定のPN値で示される位置でカットしてローテーションすることにより暗号化した波形は第8図Bのようなものとなる。従って、その鍵 K_t により初期のPN値が決定できれば、第8図Bの暗号化映像信号を復号してAへ戻すことは容易である。

ここで、復号化(デスクランブル)に用いる鍵

K_1 が1週間単位で変更されるものとする、上述したような受信及び記録に用いた有料デコーダを用いてVTRから再生しても、一週間後にはその鍵 K_1 が変更されていて第5図中の K_1 メモリA16の鍵 K_1 は記録時のものとは異なっている。従って、このような場合にはVTRの再生信号から K_1 を得る必要がある。又、上述のように、記録時に鍵 K_1 を鍵 K_2 を用いて暗号化しているので、録画時に用いた有料デコーダ以外の有料デコーダを用いてもその鍵 K_1 を有していないためにはや鍵 K_1 が得られないことになり、再生信号のスクランブルを解くことはできない。

なお、鍵 K_1 が変化していないことが判っているときには、第5図の構成において再生時に K_1 メモリB30の出力を用いずに、 K_1 メモリA16の出力を用いてデスクランブル処理部32で再生信号をデスクランブルするように改造することにより、鍵 K_1 が次に変更されるまでは再生信号から復号化した K_1 を用いなくても、すなわち K_1 を用いなくても再生信号をデスクランブルすることが可能にな

物理的に阻止して改造を防止できる。

次に、上述したような鍵 K_1 の暗号化(スクランブル化)の具体的な内容と、暗号復号化回路15の動作について、第6, 7図を用いて補足説明する。ここでは、鍵 K_1 の更新周期を毎週1回とし、夜間に行なうものとする。なお、有料デコーダ端末の電源が切断されていると有料デコーダ内の K_1 メモリA16の K_1 を更新できないので、念のため毎日深夜に鍵 K_1 を鍵 K_2 で暗号化して各端末の有料デコーダへ送るものとする。仮に、音声データ信号のQPSK変調信号を用いて各種データを送るものとし、その毎秒2.048Mビット中の500Kビットを鍵 K_1 の配送に使うものとする。また、1端末当りの鍵 K_1 を32ビットとし、アドレスを24ビットとすると、1端末当たり56ビット必要である(第7図参照)。また、伝送する1パケットを、ヘッダを含めて第8図の如く288ビットとする。Aは識別番号1が付された各種制御情報のパケット、Bは識別番号2が付され K_1 を含む制御番号用のパケットである。272ビットを文

てしまう。つまり、固有の鍵 K_1 を有していない有料デコーダでも、伝送信号から K_1 を取り出すことができるものであれば、鍵 K_1 で暗号化して記録した信号を再生することができる。つまり、実質的な盗視聴が可能になる。このようなことを防ぐには、鍵 K_1 を比較的短期間で変化更すること、及び、第5図の有料デコーダにおいてVTR再生指示がされたときに K_1 メモリA16から読み出した鍵 K_1 によってデスクランブルすることが簡単にできないように、この切換部を改造できない構造にすることにより、同一の有料デコーダによる個人的な記録再生以外をできなくすることができ、不法な複製テープの作成を阻止できる。第9図はそのような構成の一例を示す。VTR再生指示回路31をスイッチ31Sとその入力を保持するメモリ31Mとにより構成し、このメモリ31Mと鍵 K_1 メモリA16、鍵 K_1 メモリB30及びセレクト30を一体化して1つのパッケージに封入するか樹脂モールドすることにより、VTR再生時に受信補助から取り出した鍵 K_1 を使用するような切換えを

字放送に使われているBEST方式による誤り訂正方式の符号化によって構成すれば、データは272ビット中の190ビットとなる。従って、一端末当たり56ビットとすると3端末分の168ビットのデータを1パケットで伝送することができる。500Kビット÷288ビット=1736が毎秒アクセスできる端末数であり、アドレスを24ビットで構成すると指定可能数は約1678万端末であるから、16,780,000÷1736=9,660万秒即ち約2.7時間で全端末をアクセスして鍵 K_1 を配送することができる。そこで、例えば月曜日の早朝2時~5時に1回鍵 K_1 を配送し、後は端末側からの要求に応じてその都度個別対応する等の方法が選べる。

第8図Bの信号形式(パケット)のQPSK変調によるデータを受信した場合、暗号復号信号15ではその識別番号が(2)であることを識別して鍵 K_1 が送られてきていることを識別し、これを自己の有する鍵 K_1 で解読し、端末アドレスと一致する暗号化された鍵 K_1 をもう一度鍵 K_1 で解読する。即ち、

鍵 K_t が二重に暗号化されているので、二重に復号化する。鍵 K_t のみ暗号化してアドレスは暗号化しない方法、鍵 K_t を他の K_i' で暗号化しておく方法もある (K_i' は端末毎に異なる K_i 以外の鍵である)。

一方、第 6 図 A の信号形式の信号を受信した場合は、暗号化回路 15 で鍵 K_t を用いて制御情報を解読し、復号化 (デスクランブル化) に必要な情報を得る。

以上は鍵の構造が第 2 図の如く二重の場合であるが、第 3 図の如く三層にすれば更に安全性が高くなる。この場合も動作は同様であるが、メモリ 16 及び 30 に鍵 K_x が記憶される点異なる。この場合、鍵 K_t は毎分あるいは毎秒単位で変更され、鍵 K_x が週、月或は年単位で変更される。鍵 K_t は第 1 図の QPSK 復調回路 13 の出力中に含まれているので、音声データ信号と共に記録され、音声データ信号と共に再生される。この場合は、第 6 図 A の制御情報は鍵 K_x で暗号化されており、鍵 K_x で復号化して得られた第 6 図 B の制御信号の中に鍵 K_t 即ち所定の PN 初期値が入っている。第 6

図のデスクランブル処理部 32 では、この PN 初期値により、映像信号や音声データ信号を復号化 (デスクランブル化) する。

発明の効果

このように、本発明によれば、暗号化した映像信号と、時間の経過により更新される鍵とを、固有の鍵によって暗号化して VTR 等により同一の記録媒体に記録するようにしているので、その記録に用いた固有の鍵を有する暗号解読装置でのみ再生し復号化することができる。従って、不正に記録した VTR テープ等の記録媒体を複写しても、その記録に使用した有料デコーダ等の暗号解読装置を用いない限り、再生して復号化 (デスクランブル化) できないので、実質的に不正コピーを防止することができる。

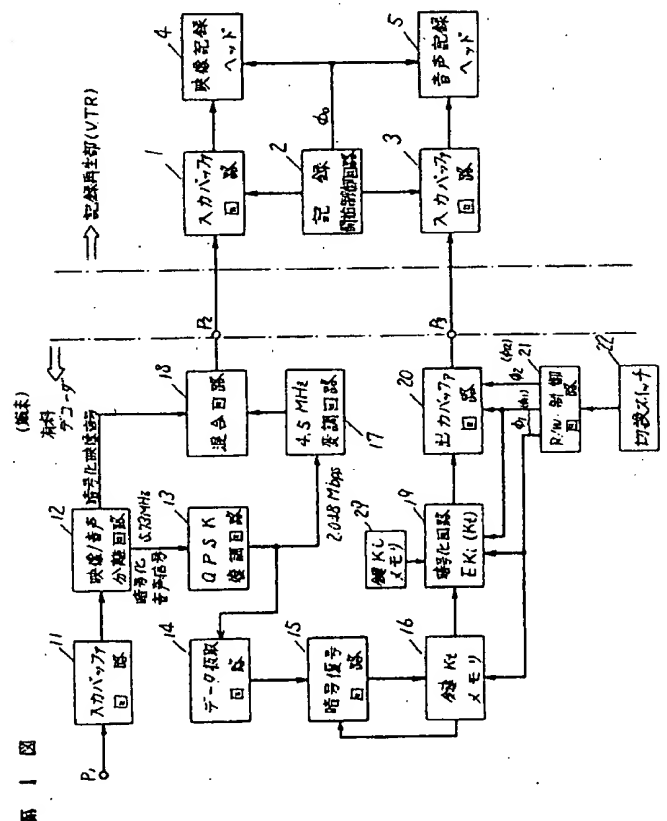
4. 図面の簡単な説明

第 1 図は本発明の一実施例における記録システムの記録部分を示すブロック図、第 2 図、第 3 図はその暗号化及び復号化の基本原理を示すブロック図、第 4 図はその記録タイミングを示すタイミ

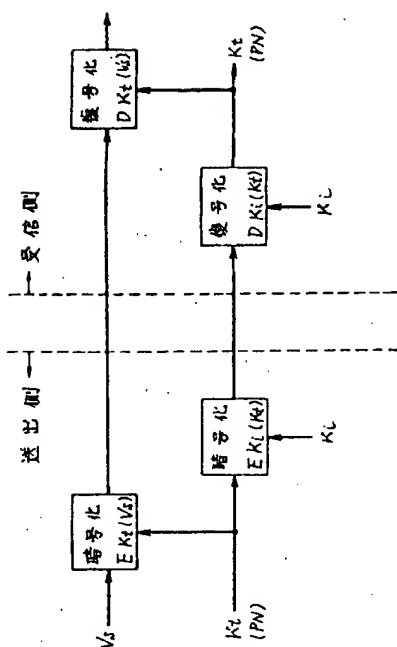
ングチャート、第 6 図は同記録システムの再生部分を示すブロック図、第 6 図、第 7 図、第 8 図は暗号化信号を示す波形図、第 9 図は本発明の他の実施例における記録システムの要部を示すブロック図である。

4 ……映像記録ヘッド、5 ……音声記録ヘッド、13 ……QPSK 復調回路、14 ……データ抜取回路、15 ……暗号復号化回路、16 …… K_t メモリ A、19 ……暗号化回路、25 ……音声検波回路、26 ……セレクトラ、28 ……復号化回路、29 …… K_t メモリ、30 …… K_t メモリ B、32 ……デスクランブル処理部。

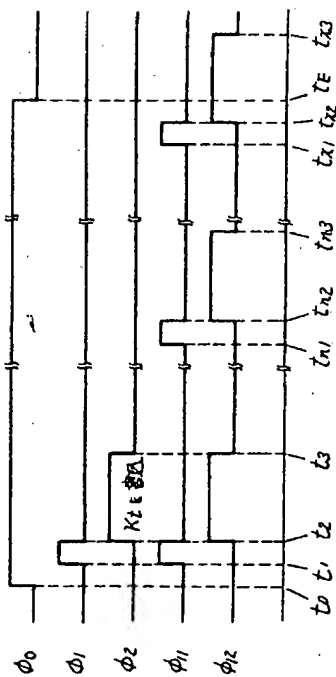
代理人の氏名 井理士 栗野重幸 ほか 1 名



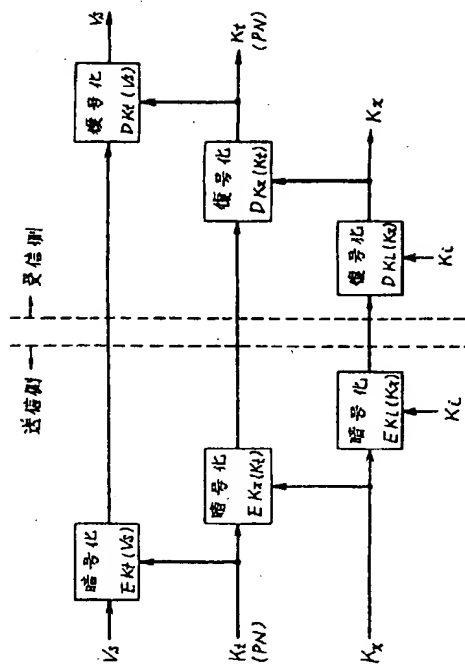
第 2 図



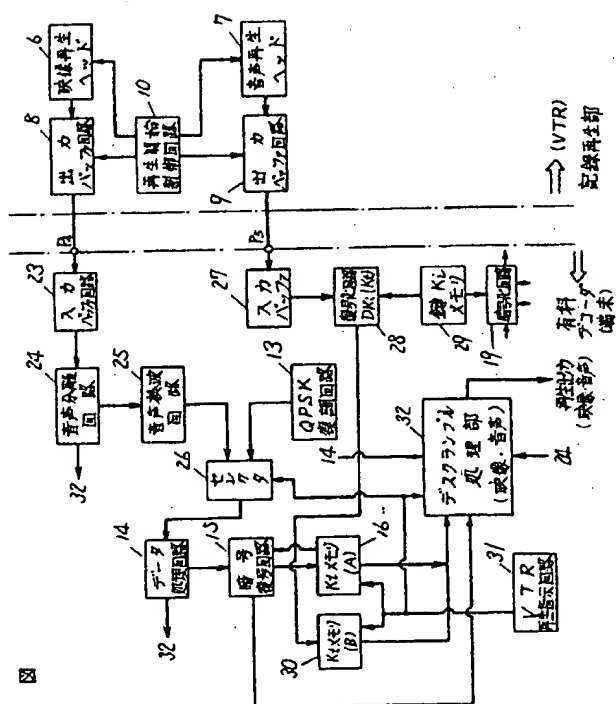
第 4 図



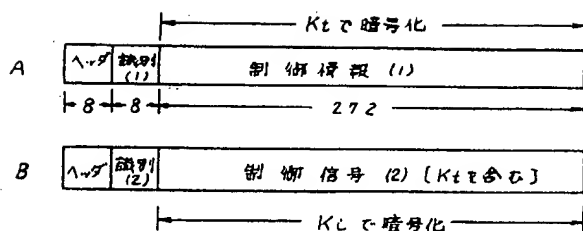
第 3 図



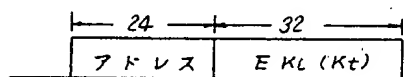
第 5 図



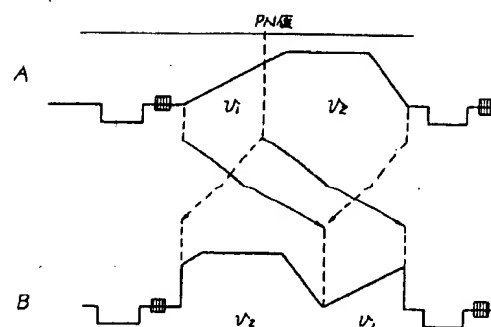
第 6 図



第 7 図



第 8 図



第 9 図

